UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/810,575	03/19/2001	Kiyohiro Obara	501.39485X00	6272

20457   7590   10/06/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/810,575	OBARA ET AL.
	Examiner	Art Unit
	Ellen C Tran	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*19 March 2001*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*1-28*</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*1-28*</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>#3 & #6</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to communication: original application filed

19 March 2001, with acknowledgement of foreign application date of 23 May 2000.

2.   Acknowledgement of Pre-Amendment filed to correct errors in specification.

3.   Claims 1-28 are currently pending in this application. Claims 1, 2, 16, 17, 18, 20,

26, and 27 are independent claims.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5.   **Claims 1-4** are rejected under 35 U.S.C. 102(e) as being anticipated by Cane et al.

U.S. Patent No. 6,754,827 (hereinafter '827).

As to independent claim 1, "A computing system being a first computing

system connected with a second computing system by a communication channel

wherein: said first computing system receives encrypted data from said second

computing system, and stores said encrypted data without decrypting" is taught in

'827 col. 3, lines 26-40.

As to independent claim 2, "A computing system being a first computing

system connected with a second computing system by a communication channel

wherein: said first computing system has a storage system, receives encrypted data

from said second computing system, and stores said encrypted data without

decrypting in said storage system" is shown in '827 col. 3, lies 26-40.

As to dependent claim 3, "wherein: said first computing system has a

network connection device, receives a cryptographic key and encrypted data from

said second computing system, and stores said encrypted data without decrypting in

said storage system" is disclosed in '827 col. 3, line 66 through col. 4, line 18.

As to dependent claim 4, "wherein: said first computing system has a

processor system, receives a cryptographic key and encrypted data from said second

computing system, and stores said encrypted data without decrypting in said

storage system" is taught in '827 col. 3, line 66 through col. 4, line 18.

6.   **Claim 26** is rejected under 35 U.S.C. 102(e) as being anticipated by Ohran U.S.

Patent No. 6,397,307 (hereinafter '307).

As to independent claim 26, "A computer system with remote copy facility

comprising: a main center consisting of a primary disk subsystem group being

connected to an upper layer device and receiving data transfer from said upper

layer device; and a remote center consisting of a secondary disk subsystem group

being connected with said primary disk subsystem group of said main center and

receiving data transfer" is taught in '307 col. 8, lines 27-40;

"wherein said primary disk subsystem group has a remote copy control

information storage component that stores control information stipulating whether

or not encrypted data transfer is performed when remote copying data to said

secondary disk subsystem group" is shown in '307 col. 5, lines 23-38;

"and performs data encryption when said control information stipulates to

perform encrypted data transfer; and said secondary disk subsystem group

confirms said control information of said primary disk subsystem group, and

performs processing appropriate to the encryption with respect to the transferred

data when said control information is to perform encrypted data transfer" is

disclosed in '307 col. 11, lines 1-8.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to be
> patented and the prior art are such that the subject matter as a whole would have been obvious at the
> time the invention was made to a person having ordinary skill in the art to which said subject matter
> pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   **Claims 5-18, 20, 24, 25, 27, and 28** are rejected under 35 U.S.C. 103(a) as being

unpatentable over '827 as applied to claims above in further view of '307.

As to dependent claim 5, the following is not taught in '827:

"**wherein: said processor system reads encrypted data from said storage**

system, decrypts it" however '307 teaches "Secondary system 14 then uses decryption

key 106b to decrypt encrypted data 110b and create decrypted data 114b" in col. 11, lines

47-49;

"**and further writes it in said storage system**" however '307 teaches "The

present invention begins with the assumption that a primary mass storage system

connected to a primary system and a secondary mass storage system connected to a

secondary system contain identical data ... by making a complete copy of the primary

mass storage system to the secondary mass storage system using either traditional ... that

need to be stored at the secondary mass storage system" in col. 5, lines 4-22.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the teachings of '827 a method or system for backing up data by

transferring it encrypted and storing the encrypted data to include a means to decrypt

and store unencrypted data. One of ordinary skill in the art would have been motivated

to perform such a modification to insure the data backup is accurate. As indicated by

'307 (see col. 4, lines 48 et seq.) "It would, therefore, represent an advancement in the

art to have a mirroring and archiving system that could ensure logical consistency of the

data protected".

As to dependent claim 6, "wherein: said network connection device reads

encrypted data from said storage system" is taught in '307 col. 7, lines "The present

invention contemplates both a system and method for mirroring and archiving a primary

mass storage system to a secondary mass storage system. The presently preferred

embodiment of the system for mirroring and archiving a primary mass storage system to

a secondary mass storage system comprises one or more general purpose computers"

"decrypts it" is shown in '307 in col. 11, lines 47-49 "Secondary system 14 then

uses decryption key 106b to decrypt encrypted data 110b and create decrypted data";

"and further writes it in said storage system" is disclosed in '307 in col. 5,

lines 4-22.

As to dependent claim 7, "wherein: said storage system reads encrypted data

within said storage system itself and decrypts and writes it" is shown in '307 in

col. 11, lines 47-49 and in col. 5, lines 4-22 "The present invention begins with the

assumption that a primary mass storage system connected to a primary system and a secondary mass storage system connected to a secondary system contain identical data ... by making a complete copy of the primary mass storage system to the secondary mass storage system using either traditional ... that need to be stored at the secondary mass storage system".

As to dependent claim 8, this claim is substantially similar to claims 5, 6, and 7; therefore it is rejected along the same rationale.

As to dependent claim 9, "wherein: reading of encrypted data from said storage system and writing of decrypted data are performed with respect to the same storage position in said storage system" is taught in '307 col. 7, lines 45-48 "The system and method of the present invention, however, can also be used with any special purpose computers or other hardware systems and all should be included within its scope".

As to dependent claim 10, "wherein: received encrypted data is stored in sequence of receipt without decryption in said storage system" is shown in '827 col. 3, lines 41-46 "The archive server then stores the encrypted file on a magnetic tape or another medium of long term storage, and stores the encrypted file key along with an index";

"and reading of encrypted data from said storage system and writing of decrypted data are such that writing is to a position being different from the position read in said storage system" is disclosed in '307 col. 8, lines 52-60 "However, the secondary mass storage keeps the updates and the initial synchronized data separate".

As to dependent claim 11, "wherein: the interval of reading of encrypted data in said first computing system is an interval of fixed time" is taught in '307 col. 8, lines 29-33 "The process begins with synchronizing the storage of both primary and secondary systems to contain identical data. Thereafter, the primary system tracks any changes made to the primary mass storage. Those changes are later consolidated, either on-the-fly or after a selected period of time".

As to dependent claim 12, "wherein: reading of encrypted data in said first computing system is started by request from the storage system in said first computing system" is shown in '307 col. 6, lines 9-16 "The present invention also includes a cache holding are in the primary mass storage system. The cache holding area retains update files so that requests for mirrored or archived data".

As to dependent claim 13, "wherein: an encryption key is received from the storage system in said first computing system" is disclosed in '827 col. 4, line 66 through col. 5, line 1 "The encrypted file 20 and encrypted key 24 are then transmitted to the archive server".

As to dependent claim 14, "wherein: an encryption key is received from the network connection device in said first computing system" is taught in '827 col. 4, line 66 through col. 5, line 1 "The encrypted file 20 and encrypted key 24 are then transmitted to the archive server".

As to dependent claim 15, this claim is substantially similar to claims 12 and 13; therefore it is rejected along the same rationale.

As to independent claim 16, "An encryption and decryption method comprising the steps of: reading encrypted data from a storage system that stores

encrypted data received in a computing system without decrypting" is taught in '827 col. 3, lines 26-40 "A computer information processing system large amounts of data are stored and must periodically be archived. Often data is copied from a source system 8 to an archive information processing system 30, hereinafter archive server, over a transmission medium, 26 and 28. The archive server 30 then copies the data to be archived onto a suitable long term storage ... at the source system encompasses encryption of the file on the source system using ... The archive server then stores the encrypted file ";

"decrypting it" is shown in '307 col. 11, lines 47-49 "Secondary system 14 then uses decryption key 106b to decrypt encrypted data 110b and create decrypted data 114b"

"and further writing it to said storage system" is disclosed in '307 col. 5, lines 4-22 "The present invention begins with the assumption that a primary mass storage system connected to a primary system and a secondary mass storage system connected to a secondary system contain identical data ... by making a complete copy of the primary mass storage system to the secondary mass storage system using either traditional ... that need to be stored at the secondary mass storage system".

As to independent claim 17, "An encryption and decryption method comprising the steps of: passing a cryptographic key to a decryption device from a storage system that stores the cryptographic key and encrypted data which is not decrypted" is taught in '827 col. 3, lines 26-40 "A computer information processing system large amounts of data are stored and must periodically be archived. Often data is copied from a source system 8 to an archive information processing system 30, hereinafter archive server, over a transmission medium, 26 and 28. The archive server 30

then copies the data to be archived onto a suitable long term storage ... at the source

system encompasses encryption of the file on the source system using ... The archive

server then stores the encrypted file ";

      "received in a computing system; sequentially sending said received

encrypted data to said decryption device" is shown in '827 col. 3, lines 41-46 "The

archive server then stores the encrypted file on a magnetic tape or another medium of

long term storage, and stores the encrypted file key along with an index";

      "decrypting it" is disclosed in '307 col. 11, lines 47-49;

      "and further writing it from said decryption device to said storage system" is

taught in '307 in col. 5, lines 4-22.

      As to independent claim 18, "A computer system with remote copy facility

comprising: a main center consisting of a primary disk subsystem group having a

control means that is connected to an upper layer device and performs sending and

receiving of data and a storage means that performs storage of said data; and a

remote center, which is disposed in a place apart from said primary disk subsystem

group, consisting of a secondary disk subsystem group having a control means and

receives encrypted data transferred from said primary disk subsystem group and a

storage means that performs storage of said transferred data" is shown in '307 col.

8, lines 27-40 "The process begins with synchronizing the storage of both primary and

secondary systems to contain identical data. Thereafter, the primary system tracks any

changes made to the primary mass storage. Those changes are later consolidated, either

on-the-fly or after a selected period of time, to reflect on the most recent change made to

each storage location of the primary mass storage ... Once created, updates from the

primary system are transferred to the secondary system through some communication link";

"**wherein said primary disk subsystem group updates a cryptographic key at a specified interval or an irregular interval, also interrupts said data transfer to said secondary disk subsystem group**" is disclosed in '827 col. 3, lines 26-46 "Referring to FIG. 1, in a computer information processing system large amounts of data are stored and must periodically be archived ... An archive transaction for a file stored at the source system encompasses encryption of the file on the source system using a secondary key, encryption of the secondary key on the source system using a master key, and transmission of the encrypted file and associated encrypted key ... and stores the encrypted file key along with an index to the tape containing the encrypted file" (i.e. "specified interval" same as "periodically be archived" / "updates a cryptographic key" same as "secondary key")

"**and transfers the updated cryptographic key to said secondary disk subsystem group**" is taught in '827 col. 3, line 66 through col. 4, line 1.

As to independent claim 20, "**A computer system with remote copy facility comprising: a main center consisting of a primary disk subsystem group having a control means that is connected to an upper layer device and performs sending and receiving of data and a storage means that performs storage of said data; and a remote center, which is disposed in a place apart from said primary disk subsystem group, consisting of a secondary disk subsystem group having a control means and receives encrypted data transferred from said primary disk subsystem group and a storage means that performs storage of said transferred data**" is shown in '307 col.

8, lines 27-40 "The process begins with synchronizing the storage of both primary and

secondary systems to contain identical data. Thereafter, the primary system tracks any

changes made to the primary mass storage. Those changes are later consolidated, either

on-the-fly or after a selected period of time, to reflect on the most recent change made to

each storage location of the primary mass storage ... Once created, updates from the

primary system are transferred to the secondary system through some communication

link";

"wherein said primary disk subsystem group, during execution of data write

processing, determines whether or not it is time for updating the cryptographic key

for encrypted data transfer, and if it is time for updating, updates said

cryptographic key" is disclosed in '827 col. 3, lines 26-46 "Referring to FIG. 1, in a

computer information processing system large amounts of data are stored and must

periodically be archived ... An archive transaction for a file stored at the source system

encompasses encryption of the file on the source system using a secondary key,

encryption of the secondary key on the source system using a master key, and

transmission of the encrypted file and associated encrypted key ... and stores the

encrypted file key along with an index to the tape containing the encrypted file" (i.e.

"specified interval" same as "periodically be archived" / "updates a cryptographic key"

same as "secondary key")

"also transfers it to said secondary subsystem assigning a sequence number

to said updated cryptographic key, and associates it with the transferred data

assigned with the sequence number" is shown in '827 col. 3, lines 41-46 "The archive

server then stores the encrypted file on a magnetic tape or another medium of long term

storage, and stores the encrypted file key along with an index";

As to dependent claim 24, "wherein: said primary disk subsystem group and

said secondary disk subsystem group are connected via a storage area network" is

disclosed in '307 col. 9, lines 6-57 "Referring now to FIG. 1, a block of one embodiment

of the of the present invention is illustrated. The system, shown generally as 10,

comprises a primary system 12, a secondary system 14, and communication link 16 for

transferring data between primary system 12 and secondary system 14. In FIG.1, primary

system 12 may be any type of networked or stand-alone computer system".

As to dependent claim 25, "wherein: data transfer between said primary disk

subsystem group and said secondary disk subsystem group is performed by

synchronous transfer or asynchronous transfer" is taught in '307 col. 10, lines 45-67

"In order to transfer data between primary system 12 and secondary system 14,

communication link 16 is used. Communication link 16 is one illustration of

communication means for transferring data between primary system 12 and secondary

system 14. Communication link 16 may comprise any combination of hardware and/or

software needed to allow data communication between primary system 12 and secondary

system 14 ... This allows communication link 16 to encompass a wider variety of

technologies that cannot be used with prior art systems"

As to independent claim 27. A remote copy method of a storage system

comprising: a local storage system that stores data written from an upper layer

device; and a remote storage system that stores a copy of said data, wherein

comprising:" is shown in '307 col. 4, lines 56-67 "The foregoing problems in the prior

state of the art have been successfully overcome by the present invention, which is

directed to a system and method for mirroring and archiving a primary mass storage

system to a secondary mass storage system";

"a step where said local storage system encrypts said data with a

cryptographic key; a step where said encrypted data is transferred from said local

storage system to said remote storage system; a step where said cryptographic key is

iteratively updated" is disclosed in '307 col. 11, lines 26-57 "The embodiment may then

use the keys generated to encrypt and decrypt some or all of the information transferred

between the systems without ever having to share the encryption key over

communication link 16. For example, primary system 12 encrypts data 108a using

encryption key 106a to generate encrypted data 110a. Encrypted data 110a is transferred

to secondary system 14 over communication link 16, resulting in encrypted data 110b.

Secondary system 14 then uses decryption key 106b to decrypt encrypted data 110b and

create decrypted data 114b. As shown in FIG. 6, secondary system 14 can send

encrypted data to primary system 12 using similar steps. Furthermore, multiple keys may

be generated without having select, exchange and manipulate additional values.

Generating multiple keys would allow primary system 12 and secondary system 14 to use

any given key for a limited time";

"and a step where said updated cryptographic key is transferred from said

local storage system to said remote storage system" is taught in '827 col. 3, line 66

through col. 4, line 1 "The encrypted file 20 and encrypted key 24 are then transmitted to

the archive server";

"wherein said encryption step uses the updated cryptographic key after said cryptographic key was updated" is shown in '307 col. 11, line 44 through col. 12, line 26 "For example primary system 12 encrypts data 108a using encryption key 106a to generate encrypted data 110a".

As to dependent claim 28, "wherein: the frequency of iteration of the step where said cryptographic key is updated is determined from the time for deciphering said cryptographic key" is disclosed in '307 col. 11, lines 50-55 "As shown in FIG. 6, secondary system 14 can send encrypted data to primary system 12 using similar steps. Furthermore, multiple keys may be generated without having select, exchange and manipulate additional values. Generating multiple keys would allow primary system 12 and secondary system 14 to use any given key for a limited time".

9.   Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over '827 in further view of '307 as applied to claims above in further view of Cannon et al. U.S. Patent No. 6,615,225 (hereinafter '225).

As to dependent claim 19, the following is not taught in the combination of '827 and '307: "wherein: said primary disk subsystem group creates data having the same data length and data pattern as data transferred to said secondary disk subsystem group, and embeds said cryptographic key in said created data" however '225 teaches "the method comprises a step of assigning a token to a base file of the primary storage site … In further steps, a copy of the base file is preferably passed from the primary site to the remote storage site" in col. 6, line 46-62.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the combination of teachings from '827 and '307 a method or system

for backing up data by transferring it encrypted and storing the encrypted data with a

means to decrypt and store unencrypted data to include a means to embed a key into the

data of the same size and description of the data being saved. One of ordinary skill in the

art would have been motivated to perform such a modification because of the number of

individual client workstations creates issues with data security. As indicated by '225 (see

col. 3, lines 16 et seq.) "One major concern in the client-server environment is that a

substantial amount of critical data may be located on client subsystems which lack the

security, reliability or care of administration that is typically applied to server

computers".

10.   **Claims 21-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over

'827 in further view of '307 as applied to claims above in further view of Kanevsky et al.

U.S. Patent No. 6,496,949 (hereinafter '949).

          As to dependent claim 21, "wherein: data encrypted and transferred from

said primary disk subsystem group to said secondary disk subsystem group is kept

without decrypting in the storage means of said remote center" is taught in '827

col. 3, lines 26-40;

the following is not taught in the combination of '827 and '307 **"and is decrypted in**

time of disaster recovery" however '949 teaches "It is a purpose of the invention to

improve computer system disaster recovery" in col. 1, lines 38-39.

          It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the combination of teachings from '827 and '307 a method or system

for backing up data by transferring it encrypted and storing the encrypted data with a means to decrypt and store unencrypted data to a method to recover from a disaster. One of ordinary skill in the art would have been motivated to perform such a modification to recover from if an emergency arises. As indicated by '949 (see col. 1, lines 125-35) "However, is an emergency arises that is more sever than a power failure, such as a fire, even the data normally stored in the computer's nonvolatile storage may be lost, permanently ... Accordingly, there is a need for disaster recovery for computer systems".

As to dependent claim 22, "wherein: when data is encrypted and transferred from said primary disk subsystem group to said secondary disk subsystem group" is taught in '307 col. 9, lines 6-57 "Referring now to FIG. 1, a block of one embodiment of the of the present invention is illustrated. The system, shown generally as 10, comprises a primary system 12, a secondary system 14, and communication link 16 for transferring data between primary system 12 and secondary system ... In this description, the term "primary" is used to refer to the fact that the system has attached mass storage means for storing a copy of the data that is to be mirrored and archived. In other words, the term "primary" is used to differentiate the system from secondary system 14. Similarly, the term "secondary" merely identifies the system with attached mass storage means for mirroring and archiving the primary system 12. Primary system 12 has attached thereto primary mass storage means for storing a plurality of data blocks in a plurality of storage locations. Each of the storage locations is specified by a unique address or other mechanism";

"said cryptographic key is remote copied to and kept at another remote center disposed in a place separate from said remote center" is shown in '827 col. 3,

lines 65 through col. 4, line 17 "The encrypted file 20 and encrypted key 24 are then

transmitted to the archive server"

"and data is decrypted using the cryptographic key kept at said other remote

center in time of disaster recovery" is disclosed in '827 col. 4, lines 18-39 "The server

then retrieves the encrypted key at step 202 and retrieves the encrypted file".

As to dependent claim 23, "wherein: when data encrypted and transferred

from said primary disk subsystem group to said secondary disk subsystem group is

decrypted, it is decrypted only when a specific portion of a record concerning said

data was searched" is disclosed in '827 col. 4, lines 18-50 "Referring to FIGS. 1 and 3,

for file recover the archive server searches the tape index disk on file 40 at step 200 to

lookup encrypted key 44 and the location of the magnetic tape volume".

Conclusion

11.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

McClain et al.   U.S. Patent No. 6,049,874   issued 04/11/2000
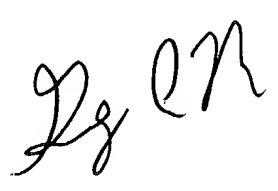
12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ellen C Tran whose telephone number is

(703) 305-8917. **"After 26 October 2004, the examiner can be reach at (571) 272-**

3842". The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
27 September 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100